



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/809,789

03/26/2004

Yoshihiro Hori

65933-082

7144

20277 7590 08/07/2008
MCDERMOTT WILL & EMERY LLP
600 13TH STREET, N.W.
WASHINGTON, DC 20005-3096

EXAMINER

GERGISO, TECHANE

ART UNIT

PAPER NUMBER

2137

MAIL DATE

DELIVERY MODE

08/07/2008

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/809,789	Applicant(s) HORI ET AL.	
	Examiner TECHANE J. GERGISO	Art Unit 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on May 27, 2008.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-3 and 12-17 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-3 and 12-17 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This is a Final Office Action in response to the applicant's' communication filed May 27, 2008.
2. Claims 1-3 and 112-17 have been examined and are pending.

Response to Arguments

3. Applicant's arguments filed May 27, 2008 have been fully considered but they are not persuasive.
4. Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

The applicant argues that Blumenau does not provide any support for the Examiner's assertion that the reference teaches "dividing a series of cryptographic processing., into a plurality of procedures," as recited in independent claim 1. However, the examiner disagrees with the applicant's argument and analysis. During examination the examiner gave the broadest reasonable interpretation to the claims in light of the applicant's disclosure. Accordingly, the examiner considered a key generation, encryption, decryption, inputting data to be encrypted, outputting the decrypted data, and any other intermediary steps in the cryptographic processing from start to end are considered as plurality of procedures. At least one or more of these procedures are inherent to any cryptographic processing. In addition these plurality of procedures

Art Unit: 2136

of cryptographic processors are also explicitly disclosed by Blumenau cited in column 38: lines 1-10, lines 53-67 and column 40: lines 20-34.

[See also the applicant's disclosure for processing procedures: 0012]

“According to its processing procedures, the cryptographic input/output processing is divided into **any of process units including**: a process for receiving data input from the host device and performing encryption or decryption using the cryptographic processing unit if necessary; a process for performing encryption, decryption, or signature attachment using the cryptographic processing unit in order to output data to the host device; and a process for outputting data to the host device. Commands may be issued by each of the process units divided.

The applicant also argues that “McClannahan does not teach that a controller of host device obtains information for estimating time necessary to execute the command from the storage device prior to the issuance of the command, sets a wait time for the command based on the obtained information, issues the command to the storage device, and waits the time set for the command before it issues a command for the next procedure to the storage device. McClannahan indicates only a delay between two operations, but does not teach, among other things, the claimed information, obtained from a storage device, for estimating time necessary to execute the command.”

Again the examiner disagrees with the applicant's argument and analysis, because McClannahan discloses the alleged features. McClannahan discloses the alleged feature recited as follows:

(McClannahan: column 3: lines 22-33; column 5: lines 12-25; column 6: lines 5-25):“The memory storage device of the type having a **predetermined timing parameter that defines a minimum delay between the first and second memory control operations**. The tuning circuit is coupled to the logic circuit and is configured to control the delay between the first and second memory control operations to meet the predetermined timing parameter for the memory storage device by cycling a programmable delay counter a selected number of clock cycles to delay performance of the second memory control operation.”

Form the above citation it is evident that a host device obtains information for estimating time necessary to execute the command from the storage device prior to the issuance of the command, sets a wait time for the command based on the obtained information.

Therefore, at least for the above reasons the applicant's arguments are not persuasive to overcome the prior arts in record and place the independent claims1, 4 and 12 in condition for allowance. Dependant claims 2, 3, 5-11 and 13-17 depending directly or indirectly from their corresponding independent claims are also not placed in condition for allowance based on their dependency.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are

Art Unit: 2136

such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 1-3 and 12-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Blumenau et al. (US Pat. No.: 6,260, 120) in view of McClannahan (US Pat. No.: 6,438, 670).

As per claim 1:

Blumenau discloses a host device operative to input data to a storage device for storing data and output data from the storage device, the host device comprising a controller which divides a series of cryptographic processing for encrypting data to be secured and inputting or outputting the same into a plurality of procedures (column 40: lines 20-34), and issues to the storage device a command for making the storage device execute a procedure to be executed on the storage-device side out of the procedures (column 35: lines 5-25; lines 53-67).

Blumenau does not explicitly teach the controller obtains information for estimating time necessary to execute the command from the storage device prior to the issuance of the command, sets a wait time for the command based on the obtained information, issues the command to the storage device, and waits the time set for the command before it issues a command for the next procedure to the storage device. McClannahan, in an analogous art, however teaches the controller obtains information for estimating time necessary to execute the command from the storage device prior to the issuance of the command, sets a wait time for the command based on the obtained information, issues the command to the storage device, and waits the time set for the command before it issues a command for the next procedure to the storage device (column 3:

Art Unit: 2136

lines 22-33; column 5: lines 12-25; column 6: lines 5-25). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the system disclosed by Blumenau to include the controller obtains information for estimating time necessary to execute the command from the storage device prior to the issuance of the command, sets a wait time for the command based on the obtained information, issues the command to the storage device, and waits the time set for the command before it issues a command for the next procedure to the storage device. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do to provide a more flexible and extensible memory controller design that is capable of supporting a wider variety of memory storage devices as suggested by McClannahan (in column 2: lines 60-66).

As per claim 2:

McClannahan discloses a host device, wherein the information for estimation includes any one of a typical processing time, an average processing time, and a maximum processing time necessary to execute the command (column 11: lines 11-20; column 5: lines 11-24).

As per claim 3:

McClannahan discloses a host device, wherein the information for estimation includes any one of a typical processing time, an average processing time, and a maximum processing time necessary for at least one basic process out of an encrypting operation, a decrypting operation, a hash operation, a random number generating operation, and log retrieval which are used to execute the command (column 5: lines 11-24; lines 30-38).

As per claim 12:

Blumenau discloses a method for executing a series of cryptographic processing for encrypting data to be secured and inputting or outputting the data between a storage device for storing data and a host device, comprising:

dividing the cryptographic processing into a plurality of procedures, and making the host device execute a procedure to be executed on the host-device side out of the procedures (column 40: lines 20-34); and

allowing the host device to issue a command to the storage device in order to make the storage device execute a procedure to be executed on the storage-device side; allowing the storage device to receive the command; and allowing the storage device to execute the command (column 28; lines 35-50, column 35: lines 5-25; Figure 33: 422-430).

Blumenau does not explicitly the host device obtains information for estimating time necessary for the storage device to execute the command from the storage device prior to the issuance of the command, issues the command to the storage device, and waits the time estimated necessary to execute the command before it issues a command for the next procedure to the storage device. McClannahan, in an analogous art, however teaches the host device obtains information for estimating time necessary for the storage device to execute the command from the storage device prior to the issuance of the command, issues the command to the storage device, and waits the time estimated necessary to execute the command before it issues a command for the next procedure to the storage device (column 3: lines 22-33; column 5: lines

Art Unit: 2136

12-25; column 6: lines 5-25). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the system disclosed by Blumenau to include the host device obtains information for estimating time necessary for the storage device to execute the command from the storage device prior to the issuance of the command, issues the command to the storage device, and waits the time estimated necessary to execute the command before it issues a command for the next procedure to the storage device. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do to provide a more flexible and extensible memory controller design that is capable of supporting a wider variety of memory storage devices as suggested by McClannahan (in column 2: lines 60-66).

As per claim 13:

Blumenau discloses a method, wherein according to the processing procedures, the cryptographic input/output processing is divided into any of process units including:

a process for receiving data input from the host device and performing encryption or decryption using the cryptographic processing unit if necessary (Figure 32: 565, 366, 79; column 37: lines 56-67; column 38: lines 55-65);

a process for performing encryption, decryption, or signature attachment using the cryptographic processing unit in order to output data to the host device (Figure 32: 565, 366, 79; column 37: lines 56-67; column 38: lines 55-65); and

a process for outputting data to the host device, and the command is issued by each of the process units divided (Figure 32: 565, 366, 79; column 37: lines 56-67; column 38: lines 55-65).

As per claims 14 and 15:

McClannahan discloses a method, wherein the information for estimation includes any one of a typical processing time, an average processing time, and a maximum processing time necessary to execute the command (column 11: lines 11-20; column 5: lines 11-24).

As per claims 16 and 17:

McClannahan discloses a method, wherein the information for estimation includes any one of a typical processing time, an average processing time, and a maximum processing time necessary for at least one basic process out of an encrypting operation, a decrypting operation, a hash operation, a random number generating operation, and log retrieval which are used to execute the command (column 5: lines 11-24; lines 30-38).

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See the notice of reference cited in form PTO-892 for additional prior art.

8. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after

Art Unit: 2136

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Contact Information

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Techane J. Gergiso whose telephone number is (571) 272-3784 and fax number is (571) 273-3784. The examiner can normally be reached on 9:00am - 6:00pm. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/T. J. G./

Application/Control Number: 10/809,789
Art Unit: 2136

Page 11

Examiner, Art Unit 2137

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2136